

ISA Server 2006 Service Pack 1 – New features and enhancements

Abstract

In this article, I will show you new and enhanced features of ISA Server 2006 Service Pack 1.

Let's begin

Many ISA Server Administrators waited a long time for the publication of ISA Server 2006 Service Pack 1. As of writing this article ISA Server 2006 Service Pack 1 is still not available as RTM, but as a Beta version.

ISA Server 2006 Service Pack 1 has many improvements above ISA Server 2006 and more new features as any other published Service Pack. The number of new features is so long that I personally call ISA Server 2006 Service Pack 1 – ISA Server 2006 R2.

The number of new and enhanced features could be the reason for the delay for publishing the next version of ISA Server 2006 – called Microsoft Forefront TMG (Thread Management Gateway).

ISA Server 2006 Service Pack 1 has the following new features:

- Configuration Change Tracking

All configuration changes of the ISA Server configuration could be saved for later review. This will give Administrators a better overview of what has been changed and if there are multiple Administrators who has changed the configuration. The Configuration change Tracking feature can also be used as a Server checklist what has changed in the ISA configuration.

- Web Publishing Rule Test Button

As most of your ISA Server Administrators know, the configuration of a secure Webserver Publishing rule with HTTPS to HTTPS or HTTP bridging could be an challenge, because many things have to be considered, you have to select correct certificates, name resolution is critical and many more. With ISA Server 2006 Service Pack 1 a new Web Publishing Rule Test Button has been integrated in ISA Server 2006 Service Pack 1 which should help you to test created Webserver Publishing rules. ISA Server will then check if the internal Server is reachable from ISA Server side and outside the Firewall.

- Traffic Simulator

The new Traffic Simulator function in ISA Server 2006 is a great feature to simulate network traffic through ISA Server 2006. The Traffic Simulator will send simulated

traffic through the ISA Server rules engine as real traffic would flow through ISA. The new Traffic Simulator could be compared with the Active Directory Group Policy feature called Group Policy results and RSOP (Resultant sets of Policies). This new feature is wonderful for us ISA Server Administrators because it let us quickly check if our rule sets works as expected.

- Diagnostic Logging Query

Diagnostic Logging query is not new to ISA Server 2006 because this feature was published in ISA Server 2004 Service Pack 3 but this feature will be enhanced in ISA Server 2006 Service Pack 1. The Diagnostic Logging Query is a feature only for concret problems related to ISA Server Firewall rules and should only be enabled for diagnostic purposes and after the problem has been resolved, the Diagnostic logging feature should be disabled, because it consumes some system resources. The Diagnostic Logging query feature in ISA Server 2006 Service Pack 1 makes it easier to see only the data that is relevant to the current troubleshooting effort.

ISA Server 2006 Service Pack 1 has the following enhancements over existing features:

- Support for Network Load Balancing (NLB) multicast and multicast with IGMP operations

ISA Server 2006 NLB clusters uses Unicast by default and this couldn't be changed until Microsoft published an update for ISA Server 2006 NLB. The use of Unicast NLB could disturb the use of bidirectional affinity (BDA). In Unicast mode, ISA nodes in an ISA Server array are all designated a single virtual IP address. The NLB driver assigns a new unicast MAC to all computers to be used by the Virtual IP (VIP). When traffic arrives the ISA Server, the switch sends all traffic to all ports. This behavior could cause in switch flooding. Multicast doesn't use this method and has some other enhancements comparing to Unicast but also some other potential pitfalls. . In multicast mode, NLB designates a multicast MAC address to all computers in the cluster. Multicast combined with Internet Group Management Protocol (IGMP) prevents all ports being flooded. The multicast support enhancement is documented in Microsoft KB article <http://support.microsoft.com/kb/938550>. The implementation of this enhancement was complex. ISA Server 2006 Service Pack 1 has this feature integrated

- Support for certificates with multiple Subject Alternative Name (SAN) entries in published web servers

The long awaited feature for all Exchange Server Administrators that have the need to publish Exchange Services like Outlook Web Access (OWA) and Outlook Anywhere must use digital certificates to secure the network traffic. Exchange Server 2007 supports the use of SAN (Subject Alternate Names) certificates – created by a Windows Server 2003 CA (SAN support must be enabled via Certutil.exe). A SAN certificate can contain more than one Server name in one certificate, so you can publish different Exchange services with only one certificate. The problem with ISA Server 2006 is that ISA Server 2006 doesn't support SAN certificates. ISA Server

2006 always uses the first name found in the certificate and ignores the rest. With ISA Server 2006 Service Pack 1 you can use SAN certificates – great!

- Kerberos Constrained Delegation (KCD) authentication supports trusted-domain user accounts

Credentials from users located in a trusted domain can now be delegated to an internal published Web site when using KCD

- RSA SecurID supports public timeout

For RSA SecurID authentication, a new form has been created that gives the user the option to select between a public or private session timeout.

- Improve Web Publishing Load Balancing (WPLB) cookie handling

ISA Server 2006 Service Pack 1 now saves the domain name of the Server to which the user is connected. ISA Server saves the domain as a cookie so that a user is not redirected to another Server within the Webserver farm.

- Filtering RPC Access rule traffic by UUID

In ISA Server 2006 without Service Pack 1 it was possible to publish RPC services based on the Universally Unique Identifier (UUID), but not within an access rule. The RPC protocol can now be added to the protocols list by selecting New RPC protocol in the Protocols option in ISA Servers toolbox so that it is possible to create outgoing access rules with filtered RPC traffic.

- Alert Improvements

ISA Server 2006 includes some new alert improvements.

New alert indicator

When a new error type alert is generated, the upper section of the details pane is now highlighted in red. This is an extremely cool feature to see which of the alarms is new to ISA Server so you doesn't have to look at the timestamp information of the alert.

New alert for logging failure

If ISA Server could not log traffic to the MSDE or local text file ISA Server enters the Lockdown mode to protect the Firewall. A new alert Indicator is triggered when the logging process takes longer than 15 seconds. This will help the ISA administrator identify logging problems before ISA Server enters the lockdown mode.

- New performance counter

A Windows performance counter has been added to measure the kilobytes per second for an HTTP/HTTPS request/response. This feature serves as an indicator to help administrators determine how to improve performance of an HTTP/HTTPS request/response process.

Change Tracking feature

Every time you change the configuration of ISA Server 2006, a dialog box opens after you click Apply to save the ISA Server policy. This dialog box gives you the chance to track the changes.

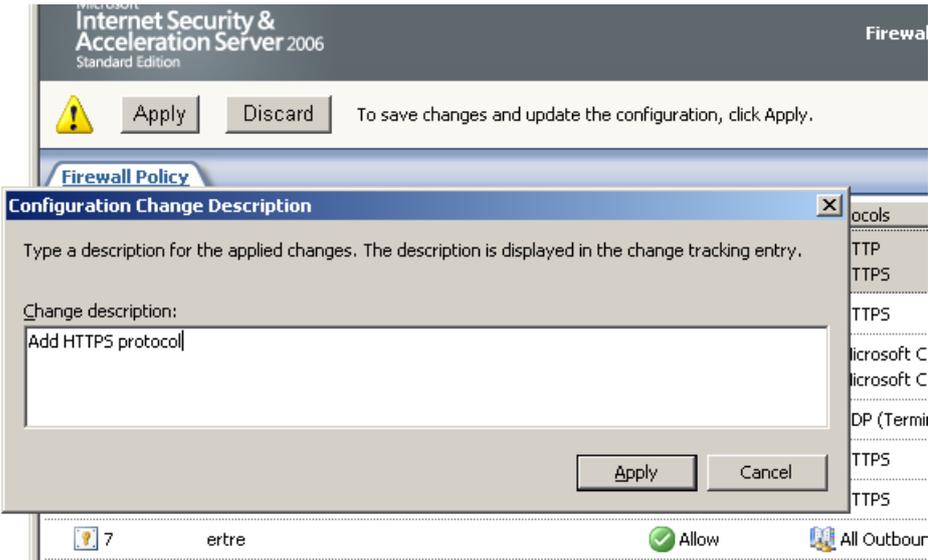


Figure 1: Configuration Change Description

You can see all changes in the ISA Server Monitoring tab called Change Tracking.

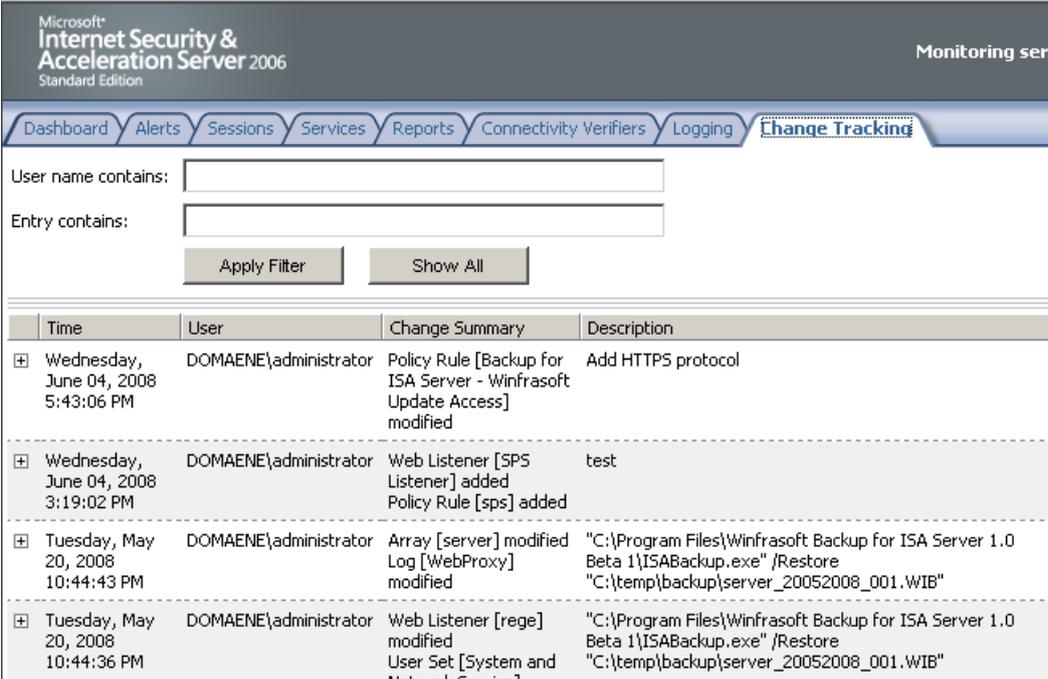


Figure 2: Change log

It is possible to enable or disable the tracking feature in the ISA console. Navigate to the ISA Servers object and click into the properties. It is also possible to limit the number of entries.

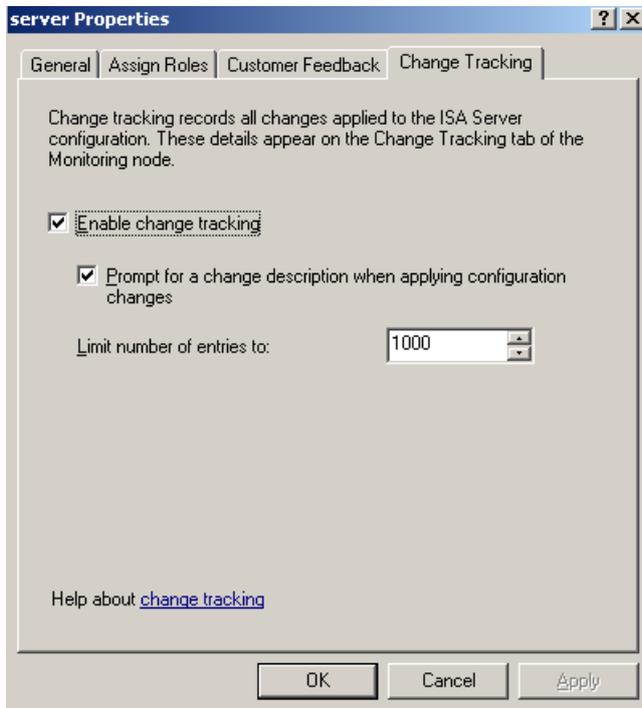


Figure 3: Enable/Disable change tracking

Web Publishing Rule Test Button

In every Publishing rule you will see a new button called Test. This new feature is used to test the functionality of the publishing rule.

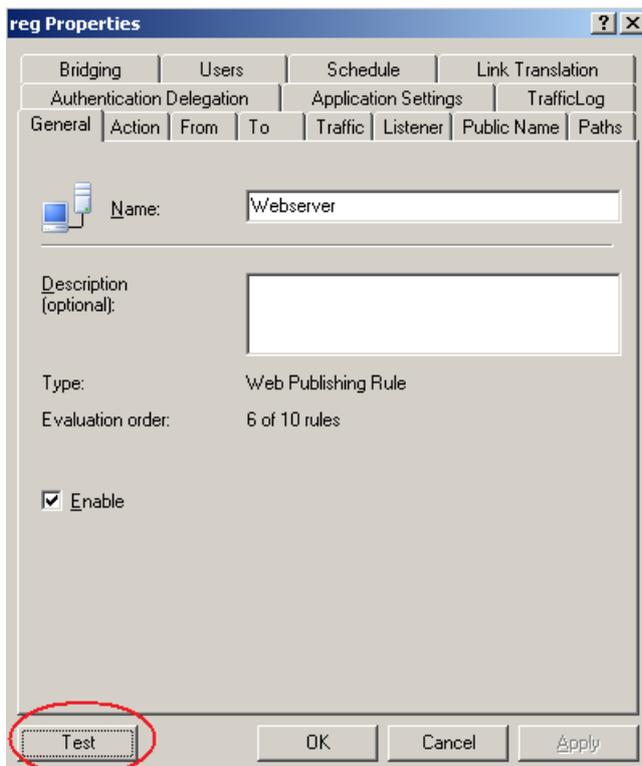


Figure 4: Test Button

If you click the test button a new window appears and you will see that ISA server tries to reach the Server and paths that you configured in the publishing rule.

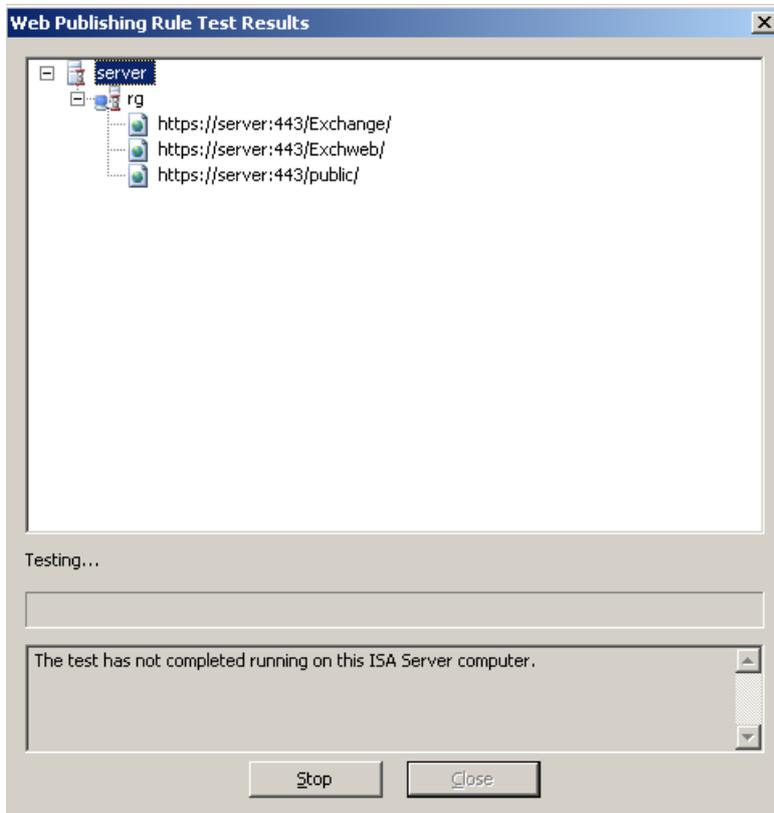


Figure 5: Web Publishing test results

Traffic simulator

The new Traffic Simulator in ISA Server 2006 Service Pack 1 lets you simulate traffic that flows through ISA Server. The Traffic Simulator is available for all Publishing and rule scenarios in ISA Server 2006.

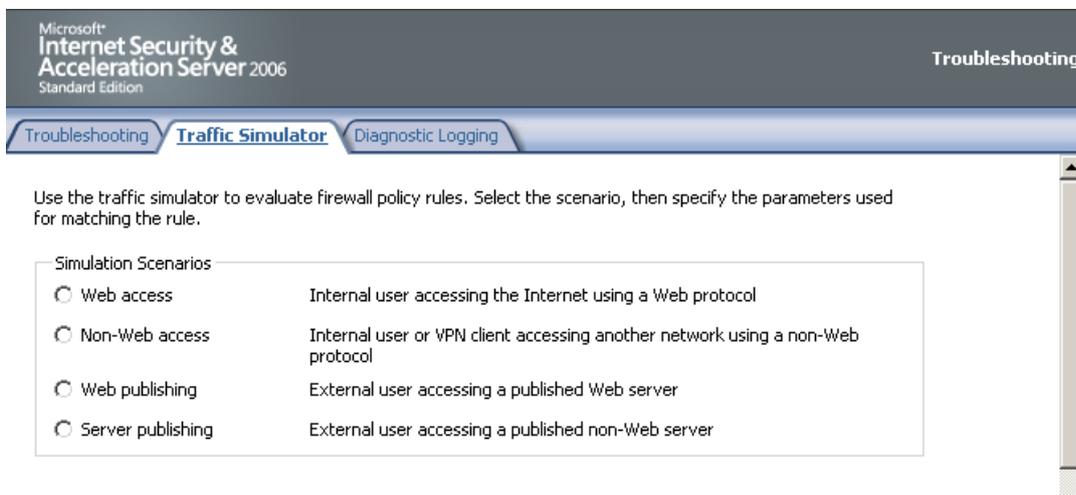


Figure 6: Traffic simulator

After you entered the required information to test, click the start button and you will see the results. In this example, the request is allowed through the Firewall rule but the name could not be resolved.

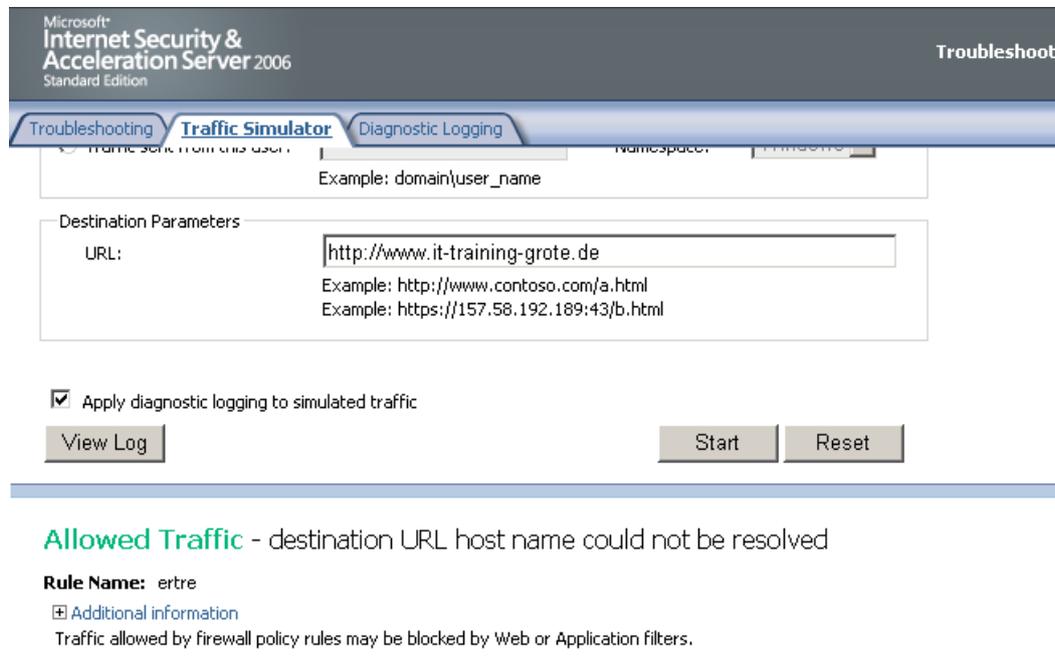


Figure 7: URL Test

Diagnostic Logging query

The Diagnostic logging query filter is now integrated into the ISA Server console and it is now easier to find informations.

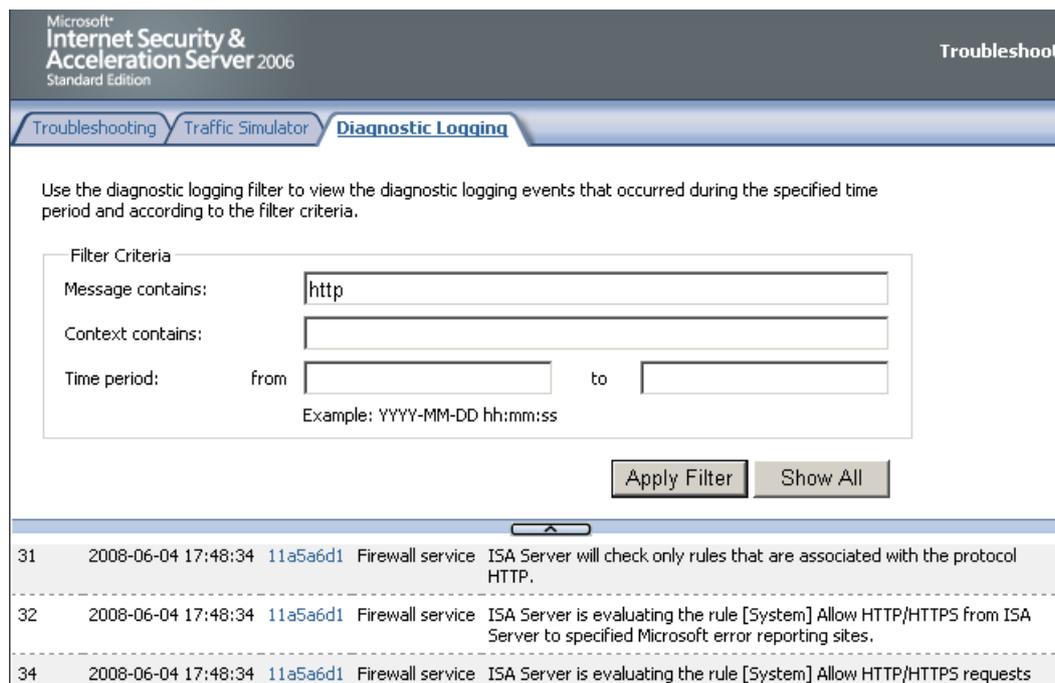


Figure 8: Enhanced Diagnostic logging

Diagnostic logging tracks the whole way through ISA Server policy components. It enhances the normal logviewer in ISA Server 2006 by tracing the flow of specific packet through the ISA rules engine. It reports on packet progress and provides information about traffic handling and rule matching.

Conclusion

In this article I explained the new and enhanced features in ISA Server 2006 Service Pack 1. ISA Server 2006 SP1 contains many new and enhanced features and this new features should give you the time to wait for the next major update from ISA Server 2006 to Microsoft Forefront TMG (Thread Management Gateway).

Related links

ISA Server 2006 SP1 Features

<http://blogs.technet.com/isablog/archive/2008/05/23/isa-server-2006-service-pack-1-features.aspx>

A user cannot access a Web site that is published in ISA Server 2006 by using Kerberos constrained delegation if the user is not in the same domain as the ISA Server computer

<http://support.microsoft.com/kb/942637/en-us>